IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA
Ft. Myers Division

JESSICA HOLT,
individually and on behalf of
others similarly situated,

Case No.

Plaintiff,

2:15-cv-691-FtM-99MRM

v.

EXPERIAN
INFORMATIONS SOLUTIONS, INC.,

Defendant.
_____/

CLASS ACTION COMPLAINT

Plaintiff, JESSICA HOLT ("Plaintiff"), brings this action on behalf of her/himself and on behalf of similarly situated persons against EXPERIAN INFORAMATION SOLUTIONS, INC., ("Experian" or "Defendant) and alleges as follows upon personal knowledge, and, as to all other matters, upon information and belief, including investigation conducted by Plaintiff's attorneys:

PRELIMINARY STATEMENT

1. Plaintiff brings this class action under Federal Rule of Civil Procedure 23, for Defendant's abject failure to safeguard Plaintiff's and Class Members' personally identifying information including dates of birth, names, addresses, Social

Security numbers ("SSNs"), and other personal information taken in a cyber-attack from Defendant Experian Information Solutions, Inc. ("Experian").

2. Plaintiff and Class Members are or were T-Mobile customers whose credit applications Experian processed from September 1, 2013, through September 16, 2015, on behalf of T-Mobile.

3. As a credit reporting agency and global data broker, Experian has a non-delegable duty to protect the personal information it maintains, necessitating its use of the most modern and robust information security protections. Data under its control has been hacked previously.

4. Nevertheless, Experian failed to safeguard Plaintiff's and Class Members' personal information adequately, in turn allowing an avenue for digital trespassers to hack Experian's computer network and steal consumers' sensitive personal information exposing them to imminent harm and risk of identity theft.

5. Experian has admitted its most recent data breach publically stating that compromised data included "name, address, Social Security number, date of birth, identification number (typically a driver's license, military ID, or passport number) and additional information used in credit assessments."[1]

6. Armed with this sensitive information alone and in combination with other data, thieves can commit a variety of crimes including, among other things,

[1] http://www.experian.com/data-breach/t-mobilefacts.html (last visited October 30, 2015).

taking out loans in another person's name; opening new financial accounts in another person's name; using the victim's information to obtain government benefits; filing a fraudulent tax return using the victim's information to obtain a tax refund; obtaining a driver's license or identification card in the victim's name but with another person's picture; or giving false information to police during an arrest.

7. As a result of the breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of fraud and identity theft.

8. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Class Members may be faced with fraudulently incurred debt. Class Members may also incur out of pocket costs for, among other things, obtaining credit reports, credit freezes, or other protective measures to deter or detect identity theft.

9. Accordingly, on behalf of herself and others similarly situated, Plaintiff sues Experian under Florida's Deceptive and Unfair Trade Practices Act for injunctive and declaratory relief, and under state and federal law, including the Fair Credit Reporting Act ("FCRA"), for statutory damages, reimbursement of out-of-pocket losses, further credit monitoring services with accompanying identity theft insurance, and improved data security.

JURISDICTION, PARTIES AND VENUE

10. All conditions precedent to the filing of this action, if any, have been performed, have occurred, or have been waived.

11. Plaintiff is natural person and citizen of Florida, residing in Lee County, Florida. Plaintiff applied for T-Mobile telephone service in or around August or September 2015, and Plaintiff's sensitive personal information was disclosed in the data breach announced by Experian, which is the subject of this action. On or about October 26, 2015, Plaintiff received a letter stating that her personal information was subject to disclosure by unauthorized persons as detailed below. *See* Exhibit A. Plaintiff is very concerned about her personal information, finances, credit, and identity and, as such, regularly monitors her credit and financial accounts, and carefully stores and disposes of personal information and other documents containing it.

12. Defendant Experian Information Solutions, Inc., is a citizen of California. It is an Ohio corporation with its headquarters and principal place of business located at 475 Anton Boulevard, Costa Mesa, CA 92626.

13. Experian is an information services company that provides data and analytical tools to clients around the world, including those located in this District. Experian collects information on people, businesses, motor vehicles, insurance, and lifestyle data, including data pertaining to United States citizens and residents.

Experian's principal lines of business are credit services, marketing services, decision analytics, and consumer services – with, among other things, a claimed expertise in fraud detection.[2]

14. Experian is registered with the Florida Secretary of State, Division of Corporations, as a foreign corporation to do business in Florida; it maintains registered an agent here; and at all times material, it engaged in substantial, continuous, systematic, and non-isolated business activity within the State of Florida, including this District.

15. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because (a) at least one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (c) none of the exceptions under the subsection apply to this action.

16. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because claims are brought under the federal Fair Credit Reporting Act, 15 U.S.C. §§ 1681e, *et seq*.

---

[2] http://www.experian.com/corporate/areas-of-expertise.html (last visited October 30, 2015). See also http://www.experian.com/corporate/fraud- detection.html (last visited October 30, 2015) (recognizing, among other things, that "[f]raud is a huge issue that is on the rise," "[t]here is a constant, ongoing battle between fraudsters and legitimate businesses, particularly in the area of digital security," "[t]here is a high social and financial cost to fraud that impacts both organizations and individuals," and "[h]undreds of fraudulent techniques exist, which include anything from theft of a credit or debit card, tax evasion, claims fraud, advertising goods and services that don't exist, falsifying information, or stealing another's identity for gain.").

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391. A substantial portion of the events and conduct giving rise to the violations alleged in this complaint occurred in this District.

FACTS APPLICABLE TO ALL COUNTS

18. Experian has touted its role and accountability as guardian of privacy and personal information. Experian has posted its privacy policy on its website, stating, in relevant part: "Experian is held accountable for its information use by consumer privacy expectations and by laws and industry codes established by government entities and industry organizations around the world…Among the laws and industry self-regulatory codes with which Experian complies in the United States are: The Fair Credit Reporting Act…"[3]

19. It further stated: "We use a variety of security systems to safeguard the information we maintain and provide. . . . . We comply with all laws and applicable self-regulatory guidelines. . . . We comply with all contractual restrictions placed on information provided to Experian."[4]

20. The implication from its privacy policy was that Experian would reasonably safeguard class members' data, and that Experian was unaware of any significant weaknesses in its data security.

[3] http://www.experian.com/privacyca/accountability.html (last accessed October 30, 2015).
[4] http://www.experian.com/privacy/information_values.html (last accessed October 30, 2015).

Hackers Gained Access to Personal Information Experian Is Admittedly Charged with Protecting

21. This however was not the case. On or about October 1, 2015, T-Mobile was notified by Experian, the vendor that processes T-Mobile's credit applications, that Experian had experienced a data breach involving its customers' personal information. According to T-Mobile, "Experian has taken full responsibility for the theft of data from its server."[5]

22. Experian maintains a historical record of the applicant data used by T-Mobile to make credit decisions. These records include personally identifiable information such as name, address and birth date, as well as encrypted fields with Social Security number and ID number (such as driver's license or passport number), and additional information used in T-Mobile's credit assessment.

23. The data Experian maintained provides the record of the applicant's credit application with T- Mobile and is used to assist with credit decisions and to respond to questions from applicants about the decision on their credit application. The data is maintained for a minimum period of 25 months. Experian explained specifically its work involving T-Mobile customers,

> In order to evaluate the risk level of a credit applicant, T-Mobile uses a variety of information to determine the likelihood that a borrower will be able to pay. Information used to do this can include a consumer's payment history, as well as information from Experian or other sources. That information is then compiled and used in their credit criteria when evaluating the risk level of an

[5] http://www.t-mobile.com/landing/experian-data-breach-faq.html (last visited October 30, 2015).

> applicant. In this case, the data acquired included the fields containing those assessments, but not the underlying information used in calculating the assessment.[6]

24. The hacker(s) acquired the records containing personal information of approximately 15 million people, including new applicants requiring a credit check for service or device financing from September 1, 2013, through September 16, 2015. Plaintiff and Class Members were among those persons whose personal information was hacked.

25. On or about October 1, 2015, Experian issued a press release stating the following in relevant part:

> [O]ne of its business units…experienced an unauthorized acquisition of information from a server that contained data on behalf of one of its clients, T-Mobile, USA, Inc. The data included some personally identifiable information for approximately 15 million consumers in the US, including those who applied for T-Mobile USA postpaid services or device financing from September 1, 2013 through September 16, 2015, based on Experian's investigation to date…
>
> …
>
> The data acquired included names, dates of birth, addresses, and Social Security numbers and/or an alternative form of ID like a drivers' license number, as well as additional information used in T-Mobile's own credit assessment. [7]

[6] http://www.experian.com/data-breach/t-mobilefacts.html ((last visited October 30, 2015).
[7] https://www.experian.com/assets/securityupdate/securityupdate-press-release.pdf ((last visited October 30, 2015).

26. "Experian determined that, although Social Security and identification numbers were encrypted, the encryption may have been compromised."[8] Experian later updated its website admitting that this information [and other personal information] was in fact downloaded by the hacker(s).[9]

Experian Has a History of Security Breaches

27. This is not the first time data maintained by the Experian group of companies has been breached. Between 2011-2012, the Privacy Rights Clearinghouse reports that an unauthorized user or users was able to access credit reporting information after managing to pass Experian's authentication process, potentially exposing consumers' names, addresses, and truncated Social Security numbers, years of birth, and account numbers exposed.[10]

28. In 2012, Experian acquired a subsidiary whose data a cyber criminal hacked and continued to hack after the purchase, exposing the Social Security numbers of 200 million Americans to the cyber black market. This breach later became the subject of class action in California.[11]

29. In addition, in 2013, the Experian group of companies suffered a prior data breach involving T-Mobile customer data. In April 2013, Experian acquired

---

[8] *Id.*
[9] http://www.experian.com/data-breach/t-mobilefacts.html (last visited October 30, 2015).
[10] https://www.privacyrights.org/node/54448
[11] *Patton, et al., v Experian Data Corp., et al.*, Case No. 8:15-cv-01142-JVS-PLA (CD CA.)

Decisioning Solutions, an identity- proofing and authentication company. Later in December 2013, Decisioning Solutions suffered a data breach in which hackers gained access to a file stored on servers Experian owned or controlled, housing Social Security numbers and driver's license numbers of T-Mobile customers.

30. Historically, Experian has not made data security a top priority:

> KrebsOnSecurity has interviewed a half-dozen security experts who said they recently left Experian to find more rewarding and less frustrating work at other corporations. Nearly all described Experian as a company fixated on acquiring companies in the data broker and analytics technology space, even as it has stymied efforts to improve security and accountability at the Costa Mesa, Calif. based firm.
>
> Jason Tate worked for a year until April 2014 as a chief information security officer delegate and risk consultant at Experian's government services and e-marketing business units. Tate said he and several of his colleagues left last year after repeatedly running into problems getting buy- in or follow-up support for major projects to beef up security around Experian's growing stable of companies handling sensitive consumer and government data.
>
> "What the board of directors at Experian wanted security-wise and the security capabilities on the ground were two completely different things," Tate said. "Senior leadership there said they were pursuing a very aggressive growth-by-acquisition campaign. The acquisition team would have a very strict protocol on how they assess whether a business may be viable to buy, but the subsequent integration of the business into our core security architecture was just a black box of magic in terms of how it was to be implemented. And I'm not saying successful magic at all."
>
> ....
>
> Not long after it acquired . . . Decisioning Solutions in April 2013, Experian folded the company into its Decision Analytics platform — a unit which provides credit and noncredit data, customer analytics and fraud detection to lenders, cable and satellite companies, telecommunications firms, third-party debt collectors, utilities and to state and federal government entities.
>
> Within hours of the latest T-Mobile breach news hitting the wires, KrebsOnSecurity was contacted by an anonymous source who sent this author

a Web link that, when clicked, opened up a support ticket within that Decision Analytics platform in the United Kingdom — with absolutely no authentication needed. That support ticket I viewed appears to have been filed by someone in an office cube at Experian's data center in Costa Rica who was requesting hardware support for a component of the company's Global Technology Services division.

....

After [the former Chief Information Officer] was lured away to take the CIO job at the Bank of England, many of the major in progress projects designed to bake security into all aspects of Experian's business ground to a halt, the former employees said on condition of anonymity. Core members of the Experian security team soon began seeking employment elsewhere. A year after [the CIO's] departure, morale suffered and the staff of the company's [security operations center] had dwindled from nearly 30 to about a dozen.

"We had a period of time there where security was viewed in a positive light, and things weren't being swept under the rug for the sake of uptime" the employee said. "[The CIO] left and it kind of went the opposite direction. Once the leadership changed, the focus changed to controlling costs and not taking systems down for maintenance, and investments started disappearing from a lot of areas. We were in the middle of putting into operation certain tools to do next-generation detection of [cyber] threats, but we weren't able to get many of them out into production. And that's how Experian wound up where they are now."[12]

31. Further, in October 2015, around the time of the Experian breach at issue here, security reported Brian Krebs exposed Experian for allowing public access to an internal portal, as follows,

> The [portal]…apparently allowed anyone to file support tickets, potentially making it easy for clever attackers who'd studied the exposed support tickets to fabricate a request for access to Experian resources or accounts on the system.

[12] Brian Krebs, *At Experian, Security Attrition Amid Acquisitions*, KREBSONSECURITY.COM, Oct. 8, 2015, http://krebsonsecurity.com/2015/10/at-experian-security-attrition-amid-acquisitions/ (last visited October 30, 2015).

> In addition, experts I spoke with who examined the portal said the support site allowed anyone to upload arbitrary file attachments of virtually any file type. Those experts said such file upload capabilities are notoriously easy for attackers to use to inject malicious files into databases and other computing environments, and that having such capability out in the open without at least first requiring users to supply valid username and password credentials is asking for trouble.[13]

Plaintiff and Class Members Suffered Common Risk and Injury

32. The risk that Plaintiff's and Class Member's personal data will be misused by the hackers who breached Experian's servers is immediate and very real. As the Attorney General of California warned, the stolen information "could be used for identity theft, particularly 'new account fraud,' or opening up new accounts in the victim's name."[14]

33. Hackers targeted Experian's server(s) in order to steal customer data, at least some of that data has been successfully decrypted, and some of the information stolen has already surfaced on websites used by hackers.

34. Defendant was and is in a superior position to know its data security capabilities, and such information is within Defendant's exclusive knowledge and not accessible to Plaintiff and Class Members. In truth and in fact, Defendant's privacy policy guaranteed the security of Plaintiff's and Class Members' personal information.

---

[13] *Id.*

[14] https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-urges-t-mobile-customers-place-fraud-alerts (last visited October 30, 2015).

35. Defendant, however, violated this guarantee and violated its legal duties to secure Plaintiff's and Class Members' personal Information. Defendant also failed to disclose the fact that the personal Information similar to Plaintiff's and Class Members' personal Information if entrusted to Defendants would not be kept securely and would be subject to identity theft while in Defendant's possession.

36. As a result of Defendant's failure to implement and follow adequate security procedures: (1) The personal information of Plaintiff and putative Class Members whom Defendant routinely gathered, maintained, and analyzed has already been stolen and traded or used by cyber criminals to commit or in attempts to commit fraud; and/or (2) Plaintiff and putative Class Members now face a substantial and imminent risk of the fraudulent use of that information, given that their information is in the hands of persons stealing the information to sell or to use in the furtherance of various frauds.

37. Class Members' personal data reportedly has already made its way to nefarious corners of the web, part of the cyber black market. On October 3, 2015, an article titled "Data Likely Stolen from Experian/T-Mobile Spotted for Sale on Dark Web" noted that Trustev, an Irish fraud-prevention company that monitors online sales of stolen data, released screen shots of listings for personal information that was likely compromised during the Experian breach. A Trustev spokesperson stated that Trustev "saw listings go up for FULLZ data that matches the same types of

information that just came out of the Experian hack." FULLZ is slang for a full package of an individual's personal identifying information including Social Security number and date of birth, among other things. The spokesperson stated that once data thieves acquire data, they typically unload it very quickly. He said it was "extremely likely" that the listings were from the Experian breach due to the "type of data and timing."[15]

38. Upon information and belief, the personal information gleaned as direct result of Experian's failure to safeguard Plaintiff's and Class Members currently in the hands of hackers in the cyber black market, which has posed an imminent risk of injury and damage to Plaintiff and Class Members,

39. Armed with this sensitive information, data thieves can commit a variety of crimes including, among other things, taking out loans in another person's name; opening new financial accounts in another person's name; using the victim's information to obtain government benefits; filing a fraudulent tax return using the victim's information to obtain a tax refund; obtaining a driver's license or identification card in the victim's name but with another person's picture; or giving false information to police during an arrest.

40. As a result of the breach, Plaintiff and Class members have been

[15] http://venturebeat.com/2015/10/03/data-likely-stolen-from-experiant-mobile-spotted-for-sale-on-dark-web-says-security-firm/ ((last visited October 30, 2015).

exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and class members must now and in the future closely monitor their financial accounts to guard against identity theft. Class members may be faced with fraudulently incurred debt. Plaintiff and Class Members may also incur out of pocket costs for, among other things, obtaining credit reports, credit freezes, or other protective measures to deter or detect identity theft.

41. Unless enjoined by the Court, this risk and injury caused by Experian will continue to injure Plaintiff and Class Members.

CLASS ACTION ALLEGATIONS

42. Plaintiff brings this class action against Defendant pursuant to Federal Rule of Civil Procedure 23(a) and 23(b)(2) and/or 23(b)(3), individually and as class representative on behalf of a class of individuals and entities, the "Class Members" or "Classes," defined as follows:

> All persons throughout the United States who were customers or potential customers of T-Mobile USA, Inc., and for which Experian performed a credit check for service or device financing from September 1, 2013, through September 16, 2015.
>
> Excluded from the Classes are Defendant, and any person, parent, subsidiary, affiliate, firm, trust, corporation, or other entity related to or affiliated with Defendant, including persons or controlled persons of Defendant, and the immediate family member of any such person.

43. Numerosity (Rule 23(a)(1)). Plaintiff alleges, on information and belief, that the number of Class Members is so numerous that joinder of them is

impractical. Experian admits that hackers stole from its server(s) the personally identifiable information for approximately 15 million consumers in the US, including those who applied for T-Mobile USA postpaid services or device financing from September 1, 2013 through September 16, 2015. The actual numbers of Class Members will be ascertained in discovery through Defendant's records as will the methods of ascertaining membership in the Classes.

44. Commonality and Predominance (Rule 23(a)(2) and Rule 23(b)(3)). Common questions of law and/or fact exist and predominate as to all members of the Class because each Class Member's claim is derived from the same data theft incident and each one's remedial claims are based on the same body of law --namely:

a. Whether Experian failed to adopt and employ adequate administrative and technical measures to ensure the security of Plaintiff's and Class Members' personal information;

b. Whether Experian's data security measures met industry standards to protect Plaintiff's and Class Members' personal information;

c. Whether Experian misrepresented or failed to accurately disclose information to customers regarding the type of security practices used;

d. Whether Experian's conduct was intentional, willful or negligent;

e. Whether Experian violated the Florida Deceptive and Unfair Trade

Practices Act;

f. Whether Experian violated the Fair Credit Reporting Act;

g. Whether Plaintiff and Class Members are entitled to declaratory and injunctive relief regarding protection of the personal information;

h. Whether Plaintiff and Class Members are entitled to damages or other monetary relief and the measure of that relief.

45. Typicality (Rule 23(a)(3)). The claims of Plaintiff are typical of the claims that would be asserted by other members of the Classes in that, in proving her claims, Plaintiff will simultaneously advance the claims of all Class Members. Plaintiff's and each Class Member's personal information was hacked while under the care and protection of Experian, which by law Experian had a duty to protect; because Experian breach the duties owed to Plaintiff and Class Members, their personal information is in the cyber black market, exposing them to immediate risk and injury; and based on the foregoing facts, Plaintiff and each Class Member has the same legal claim for violation of statutory and common law.

46. Adequacy (Rule 23(a)(4)). Plaintiff will fairly and adequately protect the interests of the Classes she represents because it is in her best interests to prosecute the claims alleged herein to obtain full redress due to her for the illegal conduct of which she complains. Plaintiff has no interests that conflict with those of the members of the Class because one or more questions of law and/or fact regarding

Defendant's liability are common to all Class Members and by prevailing on her own claims, Plaintiff necessarily will establish Defendant's liability to other Class Members.

47. Plaintiff has retained counsel experienced in litigating complex class actions. Plaintiff's counsel are long-standing members of the Florida Bar, whose practices focus on state and federal consumer, privacy, and class litigation in Florida and in other state and federal jurisdictions. Counsel have the necessary financial resources to adequately and vigorously litigate this class action, and Plaintiff and her counsel are aware of their fiduciary responsibilities to Class Members and are determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for the Classes defined above.

48. Superiority (Rule 23(b)(3)). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The detriment suffered individually by Plaintiff and the other Class Members is relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impractical for Rule 23(b)(3) Class Members to individually seek redress for Defendant's wrongful conduct. Even if these Class Members could afford individual litigation, the court system could not. Individualized litigation creates the potential

for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class-action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. It makes no sense for the same issues with respect to Defendant's conduct to be heard and decided by separate courts. Uniformity of decisions will be ensured through class treatment of this case.

49. Rule 23(b)(2). The prerequisites for maintaining the Class for injunctive and equitable relief pursuant to Federal Rule of Civil Procedure 23(b)(2) are satisfied because Defendant has acted or refused to act on grounds generally applicable to the Class thereby making appropriate final injunctive and equitable relief with respect to the Class as a whole. Defendant's actions are generally applicable to the Class as a whole and make equitable remedies, including declaratory relief, with respect to the Class as a whole appropriate.

50. The litigation of Plaintiff's claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

51. Adequate notice can be given to Class Members directly using information maintained in Defendant's records and through publication.

COUNT I
Willful Violation of the Fair Credit Reporting Act
(15 U.S.C. § § 1681, *et seq.*)

52. Paragraphs 1-51 are re-alleged and incorporated herein.

53. Under 15 U.S.C. § 1681a(f), a "consumer reporting agency" includes any person which, for monetary fees or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other consumer information for the purpose of furnishing "consumer reports" to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

54. Pursuant to 15 U.S.C. § 1681a(d)(1), a "consumer report" is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used, expected to be used, or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for (i) credit or insurance to be used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) any other purpose authorized by 15 U.S.C. § 1681b.

55. "Consumer credit information" includes, inter alia, a person's name, identification number (e.g., Social Security number), marital status, physical address and contact information, educational background, employment, professional or

business history, financial accounts and financial account history (i.e., details of the management of the accounts), credit report inquiries (i.e., whenever consumer credit information is requested from a credit reporting agency), judgments, administration orders, defaults, and other notices.

56. FCRA limits the dissemination of "consumer credit information" to certain well- defined circumstances and no others. 15 U.S.C. § 1681b(a).

57. At all relevant times, Experian was (and continues to be) a consumer reporting agency under FCRA because, on a cooperative, nonprofit basis and for monetary fees, it regularly (i) received, assembled and/or evaluated Plaintiff's and class members' "consumer credit information" protected by FCRA for the purpose of furnishing consumer reports to third parties, and (ii) used the means and facilities of interstate commerce to prepare, furnish and transmit consumer reports containing Plaintiff's and class members' consumer credit information to third parties (and continues to do so).

58. As a consumer reporting agency, Defendant was (and continues to be) required to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard, protect and limit the dissemination of consumer credit information in its possession, custody and control, including Plaintiff's and class members' consumer

credit information, only for permissible purposes under FCRA. See 15 U.S.C. § 1681(b).

59. By its wrongful actions, inaction and omissions, want of ordinary care, and the resulting security breach, Defendant willfully and recklessly violated 15 U.S.C. § 1681(b), 15 U.S.C. § 1681a(d)(3), 15 U.S.C. § 1681b(a);(g), and 15 U.S.C. § 1681c(a)(6) (and the related applicable regulations) by failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and class members' consumer credit information.

60. Defendant's wrongful actions, inaction and omissions, and want of ordinary care, in turn, directly and proximately caused the security breach which, in turn, directly and proximately resulted in the wrongful dissemination of Plaintiff's and class members' consumer credit information into the public domain for no permissible purpose under FCRA. Defendant's willful and reckless FCRA violations also have prevented it from timely and immediately notifying Plaintiff and class members about the security breach which, in turn, inflicted additional economic damages and other actual injury and harm on Plaintiff and Class Members.

61. Defendant's wrongful actions, inaction, omissions, and want of ordinary care, and the resulting security breach, directly and proximately caused Plaintiff and class members to suffer economic damages and other actual injury and

harm, and collectively constitute the willful and reckless violation of FCRA. Had Defendant not engaged in such wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and class members' consumer credit information would not have been disseminated to the world for no permissible purpose under FCRA, and used to commit identity fraud. Plaintiff and class members, therefore, are entitled to declaratory relief (as set forth below), injunctive relief (as set forth below), and compensation for their economic damages, and other actual injury and harm in the form of, inter alia, (i) the lost intrinsic value of their privacy, (ii) deprivation of the value of their consumer credit information, for which there is a well-established national and international market, (iii) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (iv) statutory damages of not less than $100, and not more than $1000, each, under 15 U.S.C. § 1681n(a)(1).

62. Plaintiff and Class Members also are entitled to recover their attorneys' fees, litigation expenses, and costs, under 15 U.S.C. § 1681n(a)(3).

63. Plaintiff has retained the counsel set forth below and has agreed to reasonably compensate them for this action on her own behalf and on behalf of all Class Members.

COUNT II
Negligent Violation of the Fair Credit Reporting Act
(15 U.S.C. § § 1681, *et seq.)*

64. Paragraphs 1-51 are re-alleged and incorporated herein.

65. In the alternative to Count I, by its wrongful actions, inaction and omissions, want of ordinary care, and the resulting security breach, Defendant negligently or in a grossly negligent manner violated 15 U.S.C. § 1681(b), 15 U.S.C. § 1681a(d)(3), 15 U.S.C. § 1681b(a);(g), and15 U.S.C. § 1681c(a)(6) (and the related applicable regulations) by failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and class members' consumer credit information.

66. Defendant's wrongful actions, inaction and omissions, and want of ordinary care, in turn, directly and/or proximately caused the security breach which, in turn, directly and proximately resulted in the wrongful dissemination of Plaintiff's and class members' consumer credit information into the public domain for no permissible purpose under FCRA. Defendant's willful and reckless FCRA violations also have prevented it from timely and immediately notifying Plaintiff and class members about the security breach which, in turn, inflicted additional economic damages and other actual injury and harm on Plaintiff and class members.

67. It was reasonably foreseeable to Defendant that its failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect

Plaintiff's and class members' consumer credit information would result in a security lapse, whereby unauthorized third parties would gain access to, and disseminate, Plaintiff's and class members' consumer credit information into the public domain for no permissible purpose under FCRA. Defendant's wrongful actions, inaction, omissions, and want of ordinary care, and the resulting security breach, directly and proximately caused Plaintiff and class members to suffer economic damages and other actual injury and harm, and collectively constitute the negligent violation of FCRA. Had Defendant not engaged in such wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and class members' consumer credit information would not have been disseminated to the world for no permissible purpose under FCRA, and used to commit identity fraud. Plaintiff and class members, therefore, are entitled to declaratory relief (as set forth below), injunctive relief (as set forth below), and compensation for their economic damages, and other actual injury and harm in the form of, inter alia, (i) the lost intrinsic value of their privacy, (ii) deprivation of the value of their consumer credit information, for which there is a well-established national and international market, and (iii) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

68. Plaintiff and Class Members also are entitled to recover their attorneys' fees, litigation expenses, and costs, under 15 U.S.C. § 1681o(a)(2).

COUNT III
Violation of FDUTPA, Chp. 501, Part II, Florida Statutes

69. Paragraphs 1-51 are re-alleged and incorporated herein.

70. This is an action for injunctive and declaratory relief pursuant to Chapter 501, Part II, Florida Statutes, the "Florida Deceptive and Unfair Trade Practices Act" ("FDUTPA").

71. Experian engages in "trade or commerce" within the meaning of FDUTPA. §501.203, Fla. Stat.

72. Section 501.204(1) of FDUTPA prohibits Defendant from engaging in "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Great weight and due consideration are to be given to the decisions of the federal courts and Federal Trade Commission in interpreting the meanings of the terms, deceptive and unfair. §501.204(2), Fla. Stat.

73. FDUTPA is meant to "protect the public...from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce.". §501.202(2), Fla. Stat.

74. FDUTPA also provides: "Without regard to any other remedy or relief to which a person is entitled, anyone aggrieved by a violation of this part may bring an action to obtain a declaratory judgment that an act or practice violates this part

and to enjoin a person who has violated, is violating, or is otherwise likely to violate this part. § 501.211(1), Fla. Stat.

75. In numerous instances through the means described above since at least 2011, Defendant failed to maintain reasonable security allowing intruders to obtain unauthorized access to the personal information of individuals, including recently, Plaintiff and Class Members. Defendant's security failure has unreasonably and unnecessarily exposed consumers' including Plaintiff's and Class Members' personal data to unauthorized access and theft.

76. Such exposure of consumers' personal information has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses. For example, Defendant's failure to implement reasonable and appropriate security measures resulted in the three data breaches stated above, the latest risking the personal information of 15 million persons.

77. All the while, Defendant has represented, directly or indirectly, expressly or by implication, that it had implemented reasonable and appropriate measures to protect the personal information of Plaintiff and Class Members against unauthorized access and use; and, Defendant has represented, directly or indirectly, expressly or by implication, that their services had a particular standard and quality, which allows them to provide a safe and secure environment for the storage and use of Plaintiff's and Class Members' personal information.

78. In truth and in fact, Defendant did not implement reasonable appropriate measures to protect the personal information of Plaintiff and Class Members against authorized access and use; and its services did not have a particular standard and quality, which allows them to provide a safe and secure environment for the storage and use of Plaintiff's and Class Members' personal information.

79. Therefore, Defendant has engaged in representations, acts, or practices that are material and likely to mislead a consumer acting reasonably under the circumstances, in violation of FDUTPA. As a result, Plaintiff and Class Members have been aggrieved.

80. Also, as set forth above, Defendants have failed to employ appropriate measures to protect the personal of Plaintiff and Class Members against authorized access and use; and failed to provide them timely notice of the data breaches that have put their information at substantial, imminent risk or actual use by criminals wanting to purchase and use the information to commit fraud.

81. Defendants' actions caused or are likely to cause substantial injury to consumers that they cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition; or Defendant's actions offend established public policy and are unethical, oppressive, unscrupulous or substantially injurious to consumers.

82. Therefore, Defendant has engaged in unfair acts or practices under FDUTPA. As a result, Plaintiff and Class Members have been aggrieved.

83. Pursuant to the FDUTPA, Plaintiff and the Class are entitled to attorney's fees, and permanent injunctive relief without proof of monetary damage, loss of profits, proof of reliance, or intent to deceive. Plaintiff and the Class seek equitable relief and to enjoin Defendant on the terms that the Court considers appropriate.

COUNT IV
Declaratory and Injunctive Relief

84. Paragraphs 1-51 are re-alleged and incorporated herein.

85. This is an action for declaratory and injunctive relief.

86. The Declaratory Judgment Act, 28 U.S.C. § 2201, allows federal courts to determine contested rights and legal relations. A declaratory judgment is often a prelude to a request for other relief, whether injunctive or monetary.

87. Plaintiff and Class Members believe that Defendant owes them a standard of care to safeguard their personal information and that they have rights arising under state and federal law to that effect. Experian has asserted that it has employed every appropriate measure to protect their information and proposed future protection, of which Plaintiff and Class Members are in legitimate doubt.

88. Upon information and believe, the personal information of Plaintiff and Class Members is currently in the hands of cyber criminals as a direct and proximate

result of Defendant's inadequate security measures, despite what it touts on this website.

89. There is a *bona fide* actual, present, practical need for the Court to determine Defendant's data security failures and their current and probably future effects on Plaintiff and Class Members, and what can be done to avoid this from happening to some 15 million persons in the US ever again.

90. The declaration requested deals with a present ascertainable state of facts as presented in the allegations set forth above.

91. Plaintiff and Class Members have actual, present, adverse and antagonistic interests to the interests of Defendant stemming from an on-going state of controversy with Defendant regarding among other things the proper method and remedies to which they are entitled to protect their personal information.

92. Plaintiff, individually, and on behalf of other similarly situated Class Members are before this Court by proper process or class representation and the relief requested is not merely a request for advice or to answer their curiosities.

93. As a result of the breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and class members must now and in the future closely monitor their financial accounts to guard against identity theft. Class members may be faced with fraudulently incurred debt. Plaintiff and Class Members may also incur out of pocket costs for,

among other things, obtaining credit reports, credit freezes, or other protective measures to deter or detect identity theft.

94. Defendant Experian's wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting security breach have caused (and will continues to cause) Plaintiff and class members to suffer irreparable harm in the form of, inter alia, economic damages and other injury and actual harm in the form of, inter alia, (i) actual identity theft and identity fraud, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy, (iv) breach of the confidentiality of their consumer reports and consumer credit information, (v) deprivation of the value of their consumer credit information, for which there is a well-established national and international market, (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (vii) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Such irreparable harm will not cease unless and until enjoined by this Court.

95. Thus, the injury detailed above will persist and remain unresolved unless the extent of Defendant's duties and consumers' rights are declared and Defendant is enjoined from continuing violation of its data security duties.

96. Any potential injury to Defendant attributable to an injunction of this course of conduct is outweighed by the irreparable injury that Plaintiffs and Class

Members and the public will suffer if such injunction is not issued; Plaintiff has no adequate remedy at law; and such injunction would not be adverse to the public interest, but in fact will serve it.

97. Plaintiff has retained the counsel set forth below and has agreed to reasonably compensate them for this action on her own behalf and on behalf of all Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, for herself and on behalf of the Class defined above, under Federal Rule of Civil Procedure 23, requests that that Court:

a. Enter a declaratory judgment finding and determining:

i. The extent of the duties Defendant owes to Plaintiff and Class Members to safeguard their personal information and the attendant rights of Plaintiff and Class Members;

ii. The length of time Defendant must offer Plaintiff and Class Members credit and other protection for their personal information;

iii. The risks and harm to which Defendant's ongoing data practices expose the personal information of Plaintiff and Class Members; and,

iv. The continuing duties Defendant owes Plaintiff and Class

Members to protect the personal information.

b. Enter an injunction requiring Experian, among other things, to:

i. Notify each person whose consumer credit information was exposed in the security breach;

ii. Provide credit monitoring to each such person for at least six years;

iii. Establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and/or identity fraud (i.e., data breach insurance), from September 16, 2015, forward to the date the above-referenced credit monitoring terminates;

iv. Engage third-party security auditors and hire security professions to assess Experian's data security and to employ expert recommendations and industry best practices to secure and safeguard the personal information of Plaintiff and Class Members; and,

v. Discontinue its wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting security breach.

c. Award Plaintiff her attorney's fees and costs and those of the Class;

d. Certify this matter as a class action under Rule 23(b)(2) and Rule 23(b)(3);

e. Appoint the undersigned as class counsel;

f. Appoint Plaintiff as class representative; and,

g. Grant any other relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff, on behalf of herself and all others similarly situated, hereby demand a trial by jury of all issues so triable in this cause.

Dated: November 3, 2015

Respectfully submitted,

/s/ Steven R. Jaffe
Steven R. Jaffe (Fla. Bar No. 390770)
E-mail: steve@pathtojustice.com
Mark S. Fistos (Fla. Bar No. 909191)
E-mail: mark@pathtojustice.com
FARMER, JAFFE, WEISSING,
EDWARDS, FISTOS & LEHRMAN, P.L.
425 N. Andrews Ave., Suite 2
Fort Lauderdale, Florida 33301
Telephone: (954) 524-2820
Facsimile: (954) 524-2822

Jennifer L. Duffy (*Pro Hac Vice Pending)*
California Bar No. 171984
E-mail: classaction.com@gmail.com
LAW OFFICES OF JENNIFER DUFFY
28649 S. Western Ave., #6571
San Pedro, CA 90734
Telephone: (310) 714-9779

Jonathan Shub (*Pro Hac Vice Pending)*
Pennsylvania Bar No. 53965
E-mail: jshub@kohnswift.com
KOHN, SWIFT & GRAF, P.C.
One South Broad Street, Suite 2100
Philadelphia, PA 19107-3304
Telephone: (215) 238-1700
Facsimile: (215) 238-1968

Attorney for Plaintiff(s)